

WHAT IS CLAIMED IS:

1. An information processing device serving as a contents using device for playing or using contents, said information processing device comprising:

a communication unit for executing communication processing with a license storage device storing rights information serving as usage rights information of contents, and communication processing with a contents distribution server;

an encryption processing unit for executing encryption processing including authentication processing in said communication processing; and

a control unit for executing processing control for inputting rights information corresponding to contents from said license storage device, via said communication unit, transmitting said input rights information to said contents distribution server, and receiving contents set corresponding to said transmission rights information from said contents distribution server and playing or using said contents.

2. An information processing device according to Claim 1, wherein said encryption processing unit has a configuration for executing verification processing for a

tampering verification value attached to contents-
corresponding rights information input from said license
storage device.

3. An information processing device according to Claim
1, wherein said encryption processing unit executes mutual
authentication with said license storage device;

and wherein said control unit has a configuration for
executing input processing of contents-corresponding rights
information input from said license storage device via said
communication unit, with the establishment of said mutual
verification as a precondition thereof.

4. An information processing device according to Claim
1, wherein said encryption processing unit has a
configuration for executing mutual authentication and key-
sharing processing with said license storage device, and for
executing verification processing for a tampering
verification value attached to contents-corresponding rights
information input from said license storage device via said
communication unit, applying a key generated in said key-
sharing processing.

5. An information processing device according to Claim
1, wherein said rights information stores download-type

information containing permit/forbid information relating to cache processing permission of distribution contents from said contents distribution server;

and wherein said control unit is of a configuration for deciding permission/forbidding of cache processing of download contents following said download type information.

6. An information processing device according to Claim 1, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said contents distribution server, and for executing verification processing for a tampering verification value attached to a contents file from said contents distribution server via said communication unit, applying a key generated in said key-sharing processing.

7. An information processing device according to Claim 1, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said contents distribution server, and for executing decryption of an encrypted contents encryption processing key attached to a contents file from said contents distribution server via said communication unit, applying a key generated in said key-sharing processing.

8. An information processing device according to Claim 1, wherein header information of a contents file received from said contents distribution server contains RHD check mode information setting whether or not to take connection with said license storage device at the time of playing contents as a precondition thereof;

and wherein said encryption processing unit executes mutual authentication processing with said license storage device for contents playing processing wherein said RHD check mode information takes connection with said license storage device at the time of playing contents as a precondition thereof;

and wherein said control unit performs contents playing processing with establishment of said authentication as a precondition thereof.

9. An information processing device according to Claim 1, wherein header information of a contents file received from said contents distribution server contains output control information of contents;

and wherein said control unit executes output control of contents following said output control information.

10. An information processing device according to

Claim 1, wherein said rights information contains contents distribution server information or index server information of a server capable of providing contents corresponding to said rights information;

and wherein said control unit is of a configuration for executing processing for deciding a connection destination following said contents distribution server information or index server information.

11. An information processing device according to Claim 1, wherein said control unit is of a configuration for executing processing for transmitting, to a contents distribution server providing contents, specs information including data format information of data formats playable at the information processing device serving as a contents using device, along with said rights information.

12. An information processing device serving as a license storage device storing rights information which is contents use rights information, said information processing device comprising:

a storage unit for storing said use rights information;

a communication unit for executing communication processing with a contents using device for playing or using contents;

an encryption processing unit for executing encryption processing including authentication processing in said communication processing via said communication unit; and

a control unit for executing output processing of contents-corresponding rights information via said communication unit with regard to said contents using device, with establishment of mutual authentication with said contents using device as a precondition thereof.

13. An information processing device according to Claim 12, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said contents using device, and for executing processing for setting a tampering verification value to rights information to be output to said contents using device, applying a key generated in said key-sharing processing.

14. An information processing device according to Claim 12, wherein said encryption processing unit executes mutual authentication with a license purchasing device which receives rights information from a license server via a network;

and wherein said control unit executes input processing of contents-corresponding rights information via said

communication unit, with establishment of said mutual authentication as a precondition thereof.

15. An information processing device according to Claim 12, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said license purchasing device, and for executing verification processing for a tampering verification value attached to contents-corresponding rights information input from said license purchasing device via said communication unit, applying a key generated in said key-sharing processing.

16. A contents distribution server for distributing contents, comprising:

a communication unit for receiving a contents use request from a contents using device, and transmitting the contents;

an encryption unit for executing encryption processing including legitimacy verification processing of contents-corresponding rights information received from said contents using device via said communication unit; and

control unit for executing output processing of a contents file via said communication unit to said contents using device, with establishment of verification of said

rights information as a precondition thereof.

17. A contents distribution server according to Claim 16, wherein said rights information contains a valid information code serving as an identification code of validity management information of said rights information; and wherein said control unit makes reference to a validity management table correlating validity information with said valid information code, and executes transmission processing of a contents file, with confirmation of the validity of the contents-corresponding rights information received from said contents using device as a precondition thereof.

18. A contents distribution server according to Claim 16, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said contents using device, and for executing processing for attaching a tampering verification value to said contents file being transmitted, applying a key generated in said key-sharing processing.

19. A contents distribution server according to Claim 16, wherein said control unit executes processing for storing, in header information of a contents file to be

transmitted to said contents using device, RHD check mode information setting whether or not to take connection with said license storage device at the time of playing contents as a precondition thereof.

20. A contents distribution server according to Claim 16, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said contents using device, and for executing encryption of a contents encryption processing key to be stored in a contents file, applying a key generated in said key-sharing processing.

21. A license server for transmitting rights information serving as contents usage rights information via a network, said server comprising:

a communication unit for executing communication processing with a requesting terminal requesting said rights information;

an encryption unit for executing encryption processing including signature generating processing with regard to rights information to be transmitted via said communication unit; and

a control unit for generating rights information storing an identifier of a license storage device serving as

a storage device for said rights information, and executing output processing of said rights information, with establishment of said mutual authentication with said requesting terminal as a precondition thereof.

22. A license server according to Claim 21, wherein said encryption processing unit has a configuration for executing mutual authentication and key-sharing processing with said requesting terminal, and for executing processing for setting a tampering verification value to rights information to be output to said requesting terminal, applying a key generated in said key-sharing processing.

23. A license server according to Claim 21, wherein said control unit executes processing for generating and transmitting rights information storing identification information of a contents distribution server or index server which distributes contents corresponding to said rights information.

24. A license server according to Claim 21, wherein said control unit generates rights information storing download type information containing permit/forbid information relating to cache processing permission of distribution contents.

25. A contents distribution system comprising:
a contents using device for playing or using contents;
a license storage device storing rights information
serving as contents usage rights information; and
a contents distribution server;

wherein said contents using device has a configuration
for inputting contents-corresponding rights information from
said license storage device, transmitting said input rights
information to said contents distribution server, and
receiving from said contents distribution server, and
playing or using, contents regarding which said transmitted
rights information have been set.

26. A contents distribution system according to Claim
25, further comprising a license server which transmits
rights information stored in said license storage device
over a network;

wherein said license storage device has a configuration
for storing rights information which said license server
transmits.

27. A contents distribution system according to Claim
25, wherein mutual authentication is executed between said
license storage device and said contents using device, and

wherein output processing of rights information from said license storage device to said contents using device is executed with establishment of said mutual authentication as a precondition thereof.

28. A contents distribution system according to Claim 25, wherein mutual authentication is executed between said contents using device and said contents distribution server, and wherein output processing of rights information from said contents using device to said contents distribution server is executed with establishment of said mutual authentication as a precondition thereof.

29. A contents distribution system according to Claim 25, wherein signature verification processing of rights information received from said contents using device is executed at said contents distribution server, and wherein transmission processing of a contents file including contents corresponding to the received rights information is executed with confirmation of the legitimacy of the received rights information by said signature verification processing as a precondition thereof.

30. An information processing method for a contents using device which plays or uses contents, said method

comprising:

a rights information input step for inputting contents-corresponding rights information from a license storage device via a communication unit;

a step for executing legitimacy verification processing of said rights information;

a rights information transmission step for transmitting the input rights information to a contents distribution server with confirmation of the legitimacy of said rights information as a precondition thereof in said legitimacy verification processing; and

a step for receiving contents set corresponding to said transmitted rights information, from said contents distribution server.

31. An information processing method according to Claim 30, further comprising:

a step for executing mutual authentication and key-sharing processing with said license storage device; and

a step for executing verification processing of a tampering verification value attached to contents-corresponding rights information input from said license storage device, applying a key generated in said key-sharing processing.

32. An information processing method according to Claim 30, further comprising:

a step for executing mutual authentication and key-sharing processing with said contents distribution server; and

a step for executing verification processing of a tampering verification value attached to a contents file from said contents distribution server, applying a key generated in said key-sharing processing.

33. A computer program which executes, on a computer system, information processing for a contents using device which plays or uses contents, said program comprising:

code for a rights information input step for inputting contents-corresponding rights information from a license storage device via a communication unit;

code for a step for executing legitimacy verification processing of said rights information;

code for a rights information transmission step for transmitting the input rights information to a contents distribution server with confirmation of the legitimacy of said rights information as a precondition thereof in said legitimacy verification processing; and

code for a step for receiving contents set corresponding to said transmitted rights information, from

- 85 -

said contents distribution server.